PKI/Secure E-mail Interoperability
Summit Results

GENERAL ISSUES

1. What are the differences between version 1 and version 2 certs and how will the version 2 cert affect email clients and browsers?

   - At the basic level, V1 uses one certificate for signing and encryption. Version 2 of the certificate will use two different certificates for email. One certificate will be for signing and the other will be for encryption. The encryption certificate will be escrowed in case the user loses their certificate.

   - Effects on email clients: Signing an email will not transfer the encryption key to the recipient. This will have to be accomplished by other means. Preliminary tests show that Microsoft email clients will be able to handle the new certs. Other email clients (e.g. Netscape, Lotus) are currently being evaluated.

2. Is it possible to publish multiple email certs to a directory? (This is a requirement for DMS client in 3.0 – users need to be able to select the correct cert.)

   - MS - Support for multiple certificates and profiles. Directory supports this, but it is unknown how the client will handle this.

3. When I log on to a secure website, what certificate do I use?

   - ID cert

4. When I get the dialogue box, how do I know what certificate to use?

   - View certificate and make sure you pick CA1 or CA2 medium id and not the one with email in the description.

   - Netscape PSM 1.2 will fix the common name problems on the certificate.

5. When are we going to start using Common Access Card (CAC) ID card, PKI cert, financial transactions? Will this change the way certs are issued or perhaps will the certs follow personnel to other commands? Will the standard ID CARD ISSUE facilities be able to handle these new cards or will they issue the card and then have an LRA import the cert. And how far are implementations combining Biometrics?

   - Can be addressed at DoD Smart Card office.

6. Has anyone come up with an automated way to delete certs out of the NT4.0 registry?

   - MS Cert Manager will do this.

   - CertUtil is available from Microsoft -Windows 2000/NT4Option Pack (Host this on MGS Page for DOD-wide use) – Will get rid of key containers.

7. What type of certificate is necessary to log onto an NT/2000 domain and why can't DoD Certificates be used for this? Does MS Certificate need to be the first certificate on a smart card (token) to be used for NT/2000 domain logon?

    - Common Access Card – Windows 2000 – Microsoft's product takes the first cert that is loaded, so if the Microsoft smart card log-on certificate is not loaded first, the log-on feature with smart cards does not work.

    - Cannot use a third party CA for use for smart card log-on.

    - Smart card log-on will not work without Active Directory.

    - Assumption was made with Smart Card Log-on – a smart card would hold a single certificate.

    - Windows 2000 – configure as an enterprise CA – logon as a very privileged user – enterprise CAs contacts has the certificates loaded that are approved – Windows 2000 CA can be subordinate to Netscape.

CONFIGURATION PKI ISSUES

1. Does IE 4.01 work on all platforms in conjunction with Outlook 98?

    - No. IE 4.01 will only work when used on NT 4 Service Pack 4 or higher. With other operating systems, Internet Explorer 5 with 128 bit encryption is required.

      Comments:

      - **SA Perspective:** Doesn't think that the end users should even know that IE4 may work. Installation is a headache for the end users, as it is with DMS, security patches that need loaded and all the minor problems that plague IE4. If some end users know that it will work in some situations and then try to install it, it can and will cause problems. Recommend that they simply are told that it is not supported and they must have at least IE5.

      - **Note from Microsoft**: Updates to the API crypto layer through service releases in NT. In order to update the API crypto layer from WIN 9x uses IE. Certificate Manager Interface (application), the update was released in IE5.

2. How are we going to address Outlook Web Access incompatibility with PKI and DMS?

    - Outlook Web Access will not work with S/MIME email. After talking with Microsoft it sounds like this will continue to be the case with Exchange 2000. So, remote users will have to use the actual mail client to be able to use PKI.

      Comments:

      - Outlook Web Access use with S/MIME e-mail is a desired capability. Microsoft should be asked to address this issue.

      - **Alternative:** What will work is MS TERMINAL SERVER with clients. It is not exactly as easy as web mail but has benefits for high end users with large .pst files or need for consistent user interface and can be run with thin clients. The connections are secured as well when combined with a PKI server cert. (Not tested in MGS Lab —submitted by Jason Hart)

3. How can PKI messages be checked for viruses?

- Virus checking of PKI enabled email should be done on the client side. Some server virus protection software may in fact corrupt signed mail. (MGS Lab pursuing issues)

  Comments:

  - **Microsoft**: Overall, this is a configuration issue / policy consideration. The Exchange server has an option "store events" to support a potential resolution for the problem.

  - SPAWAR uses the TREND product (Scan Mail for Exchange?) and have not experienced any of these problems.

  - The problem with this is that the server has to be able to decode (which I believe would open up a security hole) the message to do this, which in the case of exchange means also the server account could possibly open it. Plus the opening of S/MIME could corrupt the digital signature. Our current view is all signatures must be updated at least every two weeks. We do install AV on the server but set not to break S/MIME.

  Actions:

  - All participants provide feedback on what products are being used and if there are any associated issues.

  - Richard Storm (Kelly AFB), Carl Hamilton (DSS), and Happy Barranco (SPAWAR Charleston) will provide server specifications to MGS Integration team.

4. What versions of Exchange Server are known to break S/MIME? Does Exchange 5.5 SP3 do this?

- Commercial Exchange 5.5 Service Pack 3 does not break S/MIME. In our test lab, as well as at some pilot sites, SP 3 is being used with no problems.

  Comments:

  - Microsoft: Not aware.
  - DOD – this is a DMS concern.

5. Will a standard NT mailbox configuration be published for DoD PKI Certs?

- TBD

<u>FUNCTIONALITY OF A CLIENT WITH PKI</u>

1. Can you extract the public key from a signed and encrypted message in Outlook?

- This works fine in Outlook 98, Outlook 2000, and Outlook 2000 SR-1.

2. Does Outlook 98 properly update contacts' certificates when the contact has already been created?

- Yes, Outlook does properly update contacts without corrupting the certificate.

3. Can a signed message be modified after it has been received in Outlook?

- Yes it can.

  Comments:

  - Outlook will only allow modification of the message body after you click reply-to.

  - You can edit the message without clicking Reply-to by selecting 'Edit Message' on the Edit pull-down menu (Outlook 2000). Without doing this, you can select portions of the message but cannot change it. Have not yet test sending a message that had been modified in this way (Emory, DoN CIO)

  - **Microsoft:** To prevent modification to a signed/unsigned message after it's been sent, set the security properties to tag the message as "confidential."

4. Does Outlook 2000 SR-1 use CertPub published certificates correctly?

- No. When a certificate has been published using CertPub, Outlook SR-1 clients do not properly pull the certificate to be used to encrypt mail. However, we believe it is possible to modify CertPub so that it works with Outlook SR-1 clients and previous versions of Outlook.

  Comments:

  - SPAWAR has double checked this and agree it is true. SPAWAR has contacted the original MS SE that wrote the VB code and he thinks it is related to some "padding" he did to the cert. He is looking at it, but has not provided any feedback yet.

  Actions:

  - Microsoft investigating with MGS Lab.

5. Do the icons sometimes incorrectly indicate either encryption or signature?

- It seems that when you reply to signed and encrypted mail with only a signed message, the reply message shows up in Outlook as encrypted. However, when you open the message it turns out the message is just signed as was originally intended. This seems to be a consistent bug with both Outlook 98 and 2000.

  Comments:

  - The same problem of an incorrect icon presentation is created when the user does not have the Outlook client configured to send "Plain Text messages with Signature Attachment". This results in a signed blob, (*.p7s format) that is binary encoded. Outlook seems to think this is an encrypted message even though it is just signed.

  - Actually this is still a bug in Outlook 2000, even SR-1. If you reply to a signed and encrypted message but only sign the reply, the icon on the receiving machine will indicate encryption. The message will still open as if it was signed.

  Actions:

  - **MS: Action**: Will resolve and provide feedback/plan for fix.

6. What has happened to a certificate when it was valid when it was sent, but is invalid when it is received?

    - The first thing to check is the time on both machines. We realize this may seem trivial but we have seen incorrect time cause this problem several times. Second, make sure that you have the correct roots loaded on your machine. Last is to make sure that there are no virus programs running on the server. There is evidence that some virus programs will try to scan encrypted mail and corrupt the message.

      Comments:

      - Suggestion for attempting to debug problem: If it is possible to obtain the raw message and pull it into a text editor, one can look for signs of corruption. It is possible to do this with Netscape, but I am not familiar with how Outlook stores messages internal to the desktop.

      Actions:

      - **Action for DISA:** Investigate and resolve issue with synchronizing the time on both CAs (Carl Hamilton)

<u>CLIENT INTEROPERABILITY</u>

1. Does the "Publish to GAL" feature in SR-1 work properly?

    - Yes, the "Publish to GAL" feature does work with Win 98, Win NT4 and Win 2000. To enable many of the features that SR-1 implements, (this is only when you upgrade to SR-1, this does not apply to clean SR-1 installs) you will need to add a registry key. This is documented in Microsoft Office 2000 SR-1 white paper.

      Comments:

      - According to Microsoft, you will also need to apply a file to your installation if you have upgraded to Outlook 2000 SR-1. If it is a clean install then nothing will need to be done to your install.

      - **Microsoft**: .reg file available.

<u>CERTIFICATE DISTRIBUTION</u>

1. Are there problems using Certpub in combination with SR-1's "Publish to GAL" feature?

    - The two can interoperate with each other. However, SR-1 does not properly pull CertPub published certificates. Outlook 98 and 2000 (without SR-1) can use "Publish to GAL" published certificates.

2. How can I make it visible to the Outlook client that a user's certificate has been published to the GAL?

    - There are two indicators that will allow the user to be able to tell if a user's certificate is published. The first is a custom attribute that will change when the cert is published. The second is a tag that can be appended to the display name so that the user can easily identify whose Cert is published.

Comments:

- With CertPub you can configure two different tags that will allow clients to know who has their certificates published. The display name can be appended to with a configurable tag, and a custom attribute is written to with another configurable tag.
- Navy uses custom attribute.
- With the "Publish to GAL" feature there is no easily visible way to determine if the user has their public key published.

Actions:

- Participants should get latest version of CertPub that has been modified by MGS.
- **MS**: Taking GAL view for action.

CLIENT DOES NOT PERFORM AS EXPECTED

1. Can you access sign and encrypted mail from non-S/MIME clients?

   - You can still read signed messages as long as they are sent in clear text form (this option is configurable in Outlook and Outlook Express). However, the message comes in the form of an attachment and is not easily accessible (especially for non-proficient computer users). Also, sending signed and/or encrypted email is not possible (this is especially apparent with Outlook Web Access and other web based email systems).

ACTION ITEMS

Microsoft recommended MGS configurations:

1. Windows 2000/Outlook 2000, SR1
2. Windows NT SP 6a/IE5/Outlook 2000,SR1
3. Windows 98, 2nd edition, IE 5.01/Outlook 2000, SR1

MGS Actions

1. Sam Schaen and MGS team will get together to look at root distribution to determine if roots can be combined into a single file. Outlook seems only to accept the first of the certificates as a root.

2. DoD PKI to offer properly configured browser that users can download.

3. Download root CA Chain for Netscape and IE browsers because the extensions are different. (Install cert tool does this (download); available on web site; must have both roots; add capability to new release.)

4. GySgt Joe Fowler, USMC, [(703) 784-3197] will provide a copy of the MS cert manager, if requested.

5. Hugh Thomas researched the status of OCSP and it will not be in Version 2.0.

6. MGS Team/DON CIO - Determine InstallCert functionality with Smart Cards.

7. Paul Friedrichs to provide further clarification on why DoD certificates must first be downloaded via Netscape and then export/import to be used by MS IE and Outlook. Paul will provide an in depth explanation with rationale regarding policy and technical issue.

8. MGS team will test the problem from the USMC MGS Pilot — when retrieving certificates from the CA (ds-1), the certificates come down 40 bit encrypted versus 128 bit encrypted when exchanged between clients — in the lab then push to vendor if needed.

9. DISA will evaluate different options on how to make acquisition of a public key transparent to the end user. This includes investigating the status of the DOD PKI PMO's plan to establish at least directory servers if not CA/directory server suites in the European and Pacific theaters.

10. Betsy Appleby will pass to PKI Policy Board the issue of establishing three time periods for the individual cert to be reissued, based on turnover. The three proposed time periods include: a temp cert for exercises or short duration access; a cert which is active for the duration of the user's tour of duty irrespective of length; and a cert which has an automatic recert period i.e. the 3 year issue.

11. Betsy Appleby will get clarification from Paul Friedrichs on what format should be the standard (LDAP, S.MIIME, etc.) and then develop a plan.

12. Betsy Appleby will provide information on the status of SIPRNET PKI and CA v1 vs. CA v2.

13. MGS will review transmission bandwidth impacts with signed/encrypted email traffic, the performance impacts of SSL server encryption, and the CPU impacts with signed/encrypted email.

14. Richard Storm and Carl Hamilton will provide Server Configuration to MGS Lab to allow MGS to research the email reply problem.

Vendor actions

1. Microsoft: SeanFi to investigate whether LDAP query can be done over SSL.

2. Microsoft to follow-up on address resolution with SPAWAR.

3. Microsoft: CRL distribution points should be established to optimize performance – local server to http – TEST SCENARIO: check how Netscape handles the Microsoft 3 distribution points for CRLs – what is in the certs? How does the Netscape client deal with this??? Microsoft to provide description of CRL distribution points – What is the exact configuration needed for Netscape email client to interoperate with the Version 2.0 PKI?

4. Netscape: Ed Hicks to provide latest White Paper on 4.2 – CRLs to address the revocation of certificates and the location of the CRLs for the Navy afloat.

5. DOD PKI WG: Is there a hard and fast requirement from DOD to have Delta CRLs and OCSP? If so, Microsoft wants to talk to GE about putting this into their product planning environment.